Amendments to the Claims

1. (ORIGINAL) A method of determining a hyperelliptic curve suitable for cryptographic purposes, comprising the steps of:

- selecting a CM field K,
- determining a representant system of all isomorphism classes of simple principally polarized Abelian varieties having complex multiplication by the maximum order in K,
- determining period matrices associated with the representant system,
- determining theta-nulls,
- determining class polynomials for the CM field over a finite field F_q,
- determining a hyperelliptic curve over the finite field F_q and
- specifying the group order n of the divisor class group of the hyperelliptic curve.

2. (ORIGINAL) A method as claimed in claim 1, wherein the hyperelliptic curve is of genus 2.

3. (ORIGINAL) A method as claimed in claim 1, wherein Igusa invariants are determined from the theta-nulls.

4. (ORIGINAL) A method as claimed in claim 3, wherein the Igusa invariants are used to determine the class polynomials.

5. (ORIGINAL) A method as claimed in claim 1, wherein Mestre invariants are determined from the theta-nulls.

6. (ORIGINAL) A method as claimed in claim 5, wherein the Mestre method is used to generate the hyperelliptic curve over F_q.

7. (CURRENTLY AMENDED) A method as claimed in ~~any of the foregoing claims~~claim 1, wherein a plurality of suitable CM fields K and the associated class

polynomials are stored in accessible form and a CM field is selected from the plurality held in store to determine the hyperelliptic curve.

8. (CURRENTLY AMENDED) A method as claimed in ~~any of the foregoing claims~~claim 1, wherein the period matrices are used in a Siegel-reduced form.

9. (CURRENTLY AMENDED) A method as claimed in ~~any of the foregoing claims~~claim 1, wherein only six theta-nulls are determined.

10. (CURRENTLY AMENDED) A method as claimed in ~~any of the foregoing claims~~claim 1, wherein, to determine the representant system, a test is not made to see whether the fundamental unit of the real subfield of the Cm field K is the norm of a unit of the CM field.

11. (CURRENTLY AMENDED) A method as claimed in ~~any of the foregoing claims~~claim 1, wherein, to determine the representant system, a set of ideal classes is determined.

12. (ORIGINAL) A method as claimed in claim 11, wherein pairs of mutually inverse ideal classes are identified and Igusa invariants are determined from the theta-nulls only once for each pair.

13. (CURRENTLY AMENDED) A method as claimed in ~~any of the foregoing claims~~claim 1, wherein q is a prime number p.

14. (ORIGINAL) A method as claimed in claim 13, wherein the prime number p is selected such that each class polynomial has no more than h_k linear factors, where h_k is the class number of the CM field K.

15. (CURRENTLY AMENDED) A method as claimed in ~~any of the foregoing claims~~claim 1, wherein the CM field is selected such that the group order n of the divisor class group of the hyperelliptic curve is exactly prime.

16. (CURRENTLY AMENDED) A method as claimed in ~~any of the foregoing claims~~claim 1, wherein q is the power of a prime number p.

17. (CURRENTLY AMENDED) A cryptographic method, wherein keys for encrypting data are determined from the group of F_q-rational numbers of a hyperelliptic curve that was generated by a method as claimed in ~~any one of the foregoing claims~~claim 1.

18. (CURRENTLY AMENDED) Cryptographic apparatus using a method according to ~~one of the preceding claims~~claim 1.

19. (ORIGINAL) Sender for sending a message, comprising a cryptographic apparatus for encrypting of messages according to claim 18.

20. (ORIGINAL) Receiver for receiving a message, comprising a cryptographic apparatus for decrypting of messages according to claim 18.